Защита ПК от несанкционированного доступа

Проблема несанкционированного доступа

Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения и/или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:

- Читать и/или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере.
- Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
- Использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети.
- Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.

Механизмы защиты ПК

Основные механизмы защиты ПК от НСД могут быть представлены:

1) физическая защита ПК и носителей информации;
2) опознавание (аутентификация) пользователей и используемых компонентов обработки информации;
3) разграничение доступа к элементам защищаемой информации;
4) криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);
5) криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки;
6) регистрация всех обращений к защищаемой информации.

Физическая защита ПК и носителей информации

ПК лучше размещать в надежно запираемом помещении, причем, в рабочее время помещение должно быть закрыто или ПК должен быть под наблюдением законного пользователя. В целях повышения надежности физической защиты в нерабочее время ПК следует хранить в опечатанном сейфе.

Опознавание (аутентификация) пользователей и используемых компонентов обработки информации

Система защиты должна надежно определять законность каждого обращения к ресурсам, а законный пользователь должен иметь возможность убедиться, что ему предоставляются именно те компоненты (аппаратура, программы, массивы данных), которые ему необходимы.

Для опознавания пользователей к настоящему времени разработаны и нашли практическое применение следующие способы:

1) с использованием простого пароля;
2) в диалоговом режиме с использованием нескольких паролей и/или персональной информации пользователей;
3) по индивидуальным особенностям и физиологическим характеристикам человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаза, фотография и некоторые другие);
4) с использованием радиокодовых устройств;
5) с использованием электронных карточек.

Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных)

Данный механизм, предназначается для обеспечения защиты информации, которая подлежит продолжительному хранению на машинных носителях.
Еще важная цель – уменьшение объемов ЗУ, занимаемых хранимой информацией.
Уменьшение объемов ЗУ достигается применением так называемых методов **сжатия данных**.

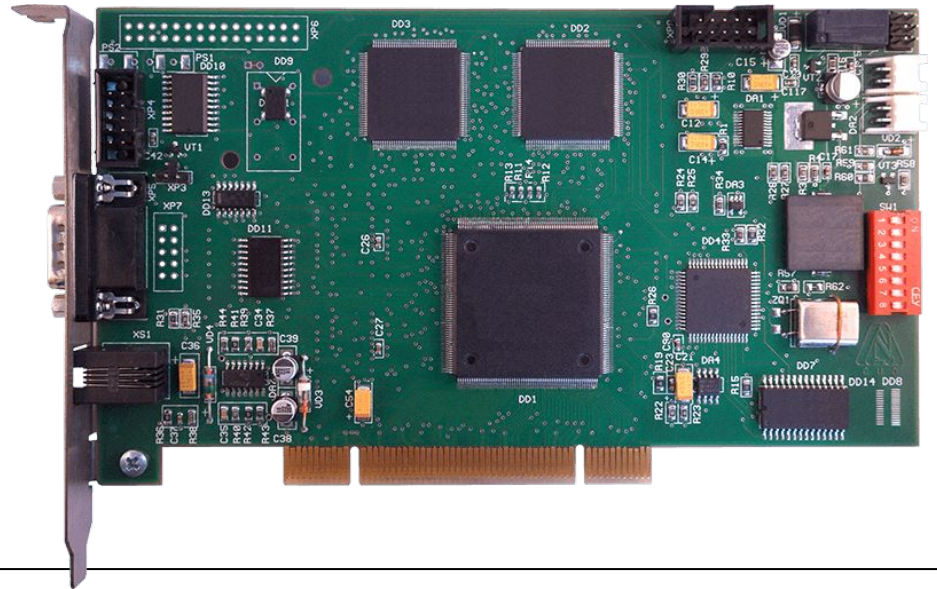
Криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки

Если обработка информации осуществляется в сетевой среде, то без применения криптографических средств надежное предотвращение несанкционированного доступа к ней практически не может быть обеспечено.

Криптографическое устройство «Криптон»

Криптон – это ряд выполняемых в виде одноплатных устройств программно-аппаратных комплексов, обеспечивающих шифрование и дешифрование информации в ЭВМ и в информационно-вычислительных сетях.

Устройство содержат датчики случайных чисел для генерации ключей и узлы шифрования, реализованные аппаратно в специализированных однокристальных микроЭВМ.



Устройство «Криптон» позволяют осуществлять:

- Шифрование и дешифрование файлов, групп файлов и разделов дисков;
- Разграничение и контроль доступа к компьютеру;
- Защиту информации, передаваемой по открытым каналам связи и сетям межмашинного обмена;
- Электронную подпись документов;
- Прозрачное шифрование жестких и гибких дисков.

Регистрация всех обращений к защищаемой информации

Регистрация обращений к защищаемой информации ПК позволяет решать ряд важных задач, способствующих существенному повышению эффективности защиты.

Основные задачи, при решении которых заметную роль играет регистрация обращений, могут быть представлены следующим перечнем:

- Контроль использования защищаемой информации;
- Выявление попыток несанкционированного доступа к защищаемой информации;
- Накопление статических данных о функционировании системы защиты.

Защита от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы

Для предотвращения такой ситуации перед оставлением компьютера необходимо либо завершить сеанс работы, либо заблокировать клавиатуру, «мышь» и экран до активизации процесса подтверждения подлинности.

Кроме того, должна быть предусмотрена возможность автоматического блокирования клавиатуры, «мыши» и экрана по истечении заданного времени бездействия пользователя.